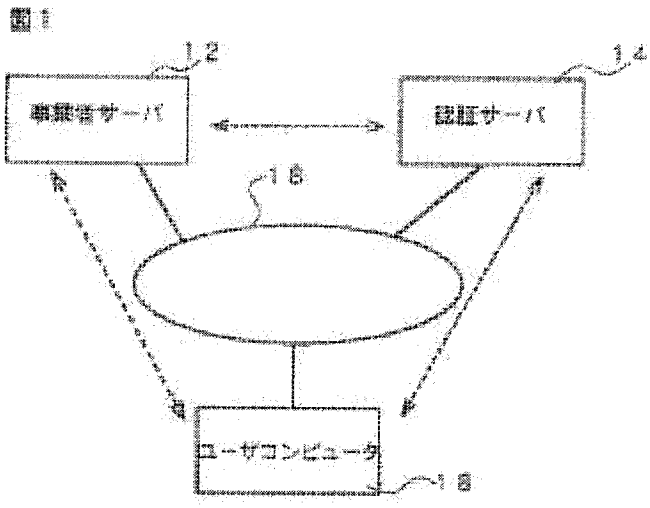
METHOD AND SYSTEM FOR AUTHENTICATING USER, USER AUTHENTICATION SYSTEM OPERATING METHOD, AUTHENTICATION SEVER AND ENTERPRISER SERVER

Publication number: JP2001306525 (A)
Publication date: 2001-11-02
Inventor(s): HORIZOE TAKESHI; AKIBA SHIGETAKA
Applicant(s): SECUGEN JAPAN LTD
Classification:
- international: ***G06Q30/00; G06F15/00; G06F21/20; G06Q10/00;*** **G06Q30/00; G06F15/00; G06F21/20; G06Q10/00;** (IPC1-7): G06F15/00; G06F17/60
- European:
Application number: JP20000126955 20000427
Priority number(s): JP20000126955 20000427

Abstract of **JP 2001306525 (A)**

PROBLEM TO BE SOLVED: To widely spread reliably authentication by means of a fingerprint collating device. SOLUTION: When a user computer 16 applies for a transaction to a enterpriser server 12, an authentication server 14 accepts the registration application of the relevant user from the dealer server 12, together with a user ID and judges whether the user owns an FPD, and when the user does not own the FPD, the FPD is imparted. Also a registration ID for registering fingerprint data utilizing the FPD is issued and transmitted to the user. When the registration ID and the fingerprint data acquired by utilizing the FPD are received from the user computer 16, the authentication server 14 stores the user ID and a dealer ID or the like in a database, while correlating them with the fingerprint data and the registration ID.; Afterwards, when the fingerprint data, the user ID and the dealer ID or the like transmitted by the user computer are received from the dealer server 12, the authentication server 14 collates the fingerprint data with fingerprint data, which are related to the user ID in the database and transmits the collation result to the enterpriser server 12.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－306525
（P2001－306525A）
(43)公開日　平成13年11月２日(2001.11.2)

(51)Int.Cl.[7]		識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ	５Ｂ０４９
		ＺＥＣ		ＺＥＣ	５Ｂ０８５
	17/60	３１０	17/60	３１０Ｅ	
		５１２		５１２	

審査請求　未請求　請求項の数９　ＯＬ　（全　９　頁）

(21)出願番号　特願2000－126955(P2000－126955)

(22)出願日　平成12年４月27日(2000.4.27)

(71)出願人　500140895
日本セキュアジェネレーション株式会社
東京都千代田区内幸町２丁目２番３号　日比谷国際ビル

(72)発明者　堀添　健
東京都千代田区内幸町２－２－３　日比谷国際ビル18Ｆ日本セキュアジェネレーション　株式会社内

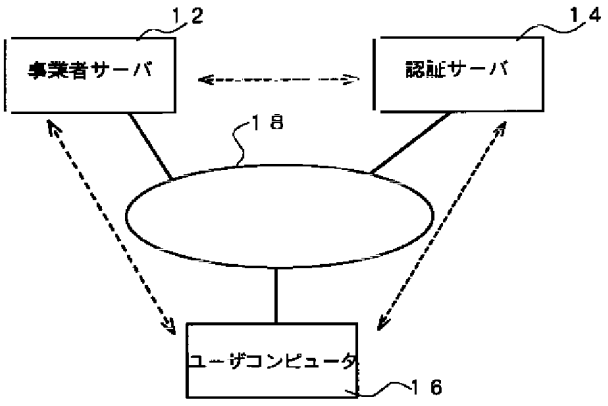
(74)代理人　100103632
弁理士　窪田　英一郎　（外１名）

最終頁に続く

(54)【発明の名称】　ユーザ認証方法、ユーザ認証システム運用方法、ユーザ認証システム、認証サーバ、および、事業者サーバ

(57)【要約】
【課題】　指紋照合装置による確実な認証を広く普及させる。
【解決手段】　ユーザコンピュータ１６が事業者サーバ１２に、取引を申請した場合に、認証サーバ１４は、事業者サーバ１２から、ユーザＩＤとともに、当該ユーザの登録申請を受理し、ユーザがＦＰＤを所持しているか否かを判断して、所持していない場合には、ＦＰＤを付与する。また、ＦＰＤを利用した指紋データの登録のための登録ＩＤを付与し、ユーザに伝達する。ユーザコンピュータ１６から、登録ＩＤとＦＰＤを利用して取得した指紋データとを受理すると、認証サーバ１４は、ユーザＩＤや事業者ＩＤ等を、指紋データおよび登録ＩＤと関連付けてデータベース中に記憶する。その後に事業者サーバ１２から、ユーザコンピュータにより伝達された指紋データ、ユーザＩＤ、事業者ＩＤ等を受理すると、認証サーバ１４は、指紋データと、データベース中の、ユーザＩＤに関する指紋データとを照合して、照合結果を、事業者サーバ１２に伝達する。

図１



【特許請求の範囲】
【請求項１】　ユーザコンピュータから、事業者或いは当該事業者の運営するサービスに関するサーバに、取引の申請があった場合に、当該サーバから、取引申請者であるユーザのユーザＩＤとともに、当該ユーザの登録の申請を受理するステップと、
前記申請の受理に応答して、当該ユーザがＦＰＤを所持しているか否かを判断して、所持していない場合には、当該ＦＰＤを付与するステップと、
ＦＰＤを利用した指紋データの登録のための登録ＩＤを付与するステップと、
ユーザコンピュータから、登録ＩＤとともにＦＰＤを利用して取得した指紋データを受理するステップと、
ユーザＩＤとともに、前記事業者に関する事業者ＩＤ、および／または、事業者の運営するサービスのサービスＩＤを、当該指紋データおよび登録ＩＤと関連付けてデータベース中に記憶するステップと、
その後に、前記サーバから、ユーザコンピュータにより伝達された指紋データおよびユーザＩＤと、事業者ＩＤおよび／またはサービスＩＤとを受理することに応答して、当該指紋データと、前記データベース中の、当該ユーザＩＤに関する指紋データとを照合するステップと、
前記照合結果を、前記サーバに伝達するステップとを備えたことを特徴とするユーザ認証方法。
【請求項２】　さらに、前記サーバから、予め指紋照合精度を示す情報を受理し、
前記データベースに記憶する際、および／または、指紋データを照合する際に、前記指紋照合精度にしたがって処理を実行することを特徴とする請求項１に記載のユーザ認証方法。
【請求項３】　ユーザコンピュータから、事業者或いは当該事業者の運営するサービスに関するサーバに取引の申請があった場合に、当該サーバから、取引申請者であるユーザのユーザＩＤとともに、当該ユーザの登録の申請を受理するステップとを備え、
前記申請の受理に応答して、当該ユーザがＦＰＤを所持しているか否かを判断して、所持していない場合には、
（ａ）当該ＦＰＤを付与するステップと、
（ｂ）ＦＰＤを利用した指紋データの登録のための登録ＩＤを付与するステップと、
（ｃ）ユーザコンピュータから、登録ＩＤとともにＦＰＤを利用して取得した指紋データを受理するステップと、
（ｄ）前記ユーザＩＤとともに、前記事業者に関する事業者ＩＤ、および／または、事業者の運営するサービスのサービスＩＤを、当該指紋データおよび登録ＩＤと関連付けてデータベース中に記憶するステップとを実行し、
既に、ユーザがＦＰＤを所持しており、かつ、上記ステップ（ａ）～（ｄ）により指紋データをデータベース中に登録している場合には、
（ｅ）前記取引の申請に添付された、ユーザを一意的に特定できる登録ＩＤに基づき、データベースを検索して、前記登録ＩＤに関連付けられたデータを見出すステップと、
（ｆ）新たな申請にかかるユーザＩＤとともに、新たな申請にかかる事業者ＩＤおよび／またはサービスＩＤを、前記登録ＩＤに関する指紋データと関連付けて前記データベース中に記憶するステップとを実行し、
その後に、前記サーバから、認証の依頼とともに、ユーザコンピュータにより伝達された指紋データおよびユーザＩＤと、事業者ＩＤおよび／またはサービスＩＤとを受理することに応答して、当該指紋データと、前記データベース中の、当該ユーザＩＤに関する指紋データとを照合するステップと、
前記照合結果を、前記サーバに伝達するステップとを備えたことを特徴とするユーザ認証方法。
【請求項４】　前記請求項１ないし３の何れか一項に記載したユーザ認証方法を利用した認証システムの運用方法であって、
前記サーバからの登録申請のたびに、前記サーバを所有する事業者或いは事業者が運営するサービスに対する初期経費を課金するステップと、
前記サーバからの認証の依頼のたびに、前記事業者或いは前記サービスに対する認証費用を課金するステップとを備えたことを特徴とする運用方法。
【請求項５】　前記ＦＰＤの費用およびその付与に伴う費用を支払うステップをさらに備えたことを特徴とする請求項４に記載の運用方法。
【請求項６】　少なくとも一以上の、事業者或いは事業者の運営するサービスに関する事業者サーバと、前記事業者サーバと接続され、ユーザの指紋データの登録およびその認証を実行する認証サーバとを備えた認証システムであって、
前記事業者サーバが、
ユーザからの登録申請があった場合に、当該ユーザにユーザＩＤを付与するユーザＩＤ付与手段と、
前記ユーザＩＤとともに、前記事業者を特定する事業者ＩＤおよび／または前記サービスを特定するサービスＩＤを前記認証サーバに伝達するＩＤ伝達手段とを有し、
前記認証サーバが、
ユーザに登録ＩＤを付与する登録ＩＤ付与手段と、
前記登録ＩＤとともにユーザから伝達された指紋データを、前記ユーザＩＤと、前記事業者ＩＤおよび／または前記サービスＩＤと関連付けて記憶するデータベースと、
前記事業者サーバとユーザとの取引の際に、前記ユーザから事業者サーバに伝達された指紋データと、ユーザＩＤと、事業者ＩＤおよび／またはサービスＩＤとを受理して、当該指紋データと、データベース中の、前記ユー

ザＩＤと事業者ＩＤおよび／またはサービスＩＤとにより特定される指紋データとを照合する照合手段とを有し、前記照合結果が、事業者サーバに伝達されるように構成されたことを特徴とする認証システム。

【請求項７】　前記認証サーバが、さらに、
前記事業者ＩＤおよび／またはサービスＩＤに対応して、認証照合精度を示すデータを記憶する照合精度記憶手段を有し、
前記データベースへの指紋データの記憶の際、および／または、前記照合手段による照合の際に、前記照合精度記憶手段に記憶された照合精度にしたがった処理を実行するように構成されたことを特徴とする請求項６に記載の認証システム。

【請求項８】　請求項６または７に記載された認証システムにおいて、指紋データの登録および照合を実行する認証サーバ。

【請求項９】　請求項６または７に記載された認証システムにおいて、前記認証システムと接続された事業者サーバ。

【発明の詳細な説明】

【０００１】

【産業上の技術分野】本発明は、電子商取引におけるユーザの認証に関し、より詳細には、ユーザに負担をかけることなく、確実にユーザを認証可能な方法に関する。

【０００２】

【従来の技術】インターネットの普及により、いわゆるオンラインショッピングが実用化されている。オンラインショッピングにおいては、支払の利便のため、クレジットカードが利用される場合が多い。或いは、購入者の銀行口座から直接、購入した費用を引き落とす手法なども提案されている。たとえば、クレジットカードにて支払う場合には、ユーザは、コンピュータを操作して、オンラインショッピングを実施しているサイトに接続し、ユーザ登録を行なう。このユーザ登録には、クレジットカード番号をサイトのサーバに伝達する一方、サーバから、ユーザＩＤが与えられる。さらに、ユーザ本人による購入であることを認証するための電子署名、暗証番号などの設定が行なわれる。このような登録手続きの後、ユーザは、サイトにて所望の商品を購入することが可能となる。商品購入の際には、ユーザはコンピュータを操作して、購入したい商品を指定するとともに、自己のクレジット番号、ユーザＩＤおよび電子署名や暗証番号をサーバに伝達する。サーバにおいては、まず、電子署名や暗証番号を用いてユーザを認証し、クレジットカードを用いた商品購入が、クレジットカードの真正な所有者によるものか否かを確認している。

【０００３】しかしながら、電子署名や暗証番号は、基本的に所定の桁数の数字の列からなるため、セキュリティの面で不完全であるという問題点があった。すなわち、クレジットカードの真正な所有者以外のものであっても、正しい数字の列さえ入力できれば、サーバは、商品の購入を許可するという問題点があった。デビットカードを用いた場合や、銀行からの直接の引き落としの場合であっても、同様の問題が起こり得る。

【０００４】そこで、指紋照合を利用して本人を認証する技術が開発されている。たとえば、本出願人が提供している指紋照合マウス（商品名「ＥｙｅＤ　マウスＩＩ」：「ＥｙｅＤ」は商標）においては、他人誤認識率０．００１％、本人排斥率０．１％という極めて高い精度にて本人の正否を認証することが可能となっている。したがって、上記指紋照合マウスなどのＦＰＤ（Finger Print Device:指紋認識装置）を利用して、ユーザ自身の指紋を登録しておけば、ユーザ以外が当該ユーザの名前を語って、不正な商取引をすること（たとえば、オンラインショッピングで商品を購入すること）を確実に防止することが可能となる。

【０００５】

【発明が解決しようとする課題】しかしながら、ユーザにとっては、指紋照合装置を購入することが求められるため、ユーザに経済的負担をかけるという問題点があった。

【０００６】本発明は、ユーザに負担をかけることなく、指紋照合装置を利用した認証システムを提供することを目的とする。また、本発明は、事業者にも過度な負担を生じさせることなく、このため、指紋照合装置による確実な認証を広く普及させることができ、これにより、電子商取引による不正を確実に防止できる認証システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の目的は、ユーザコンピュータから、事業者或いは当該事業者の運営するサービスに関するサーバに、取引の申請があった場合に、当該サーバから、取引申請者であるユーザのユーザＩＤとともに、当該ユーザの登録の申請を受理するステップと、前記申請の受理に応答して、当該ユーザがＦＰＤを所持しているか否かを判断して、所持していない場合には、当該ＦＰＤを付与するステップと、ＦＰＤを利用した指紋データの登録のための登録ＩＤを付与するステップと、ユーザコンピュータから、登録ＩＤとともにＦＰＤを利用して取得した指紋データを受理するステップと、ユーザＩＤとともに、前記事業者に関する事業者ＩＤ、および／または、事業者の運営するサービスのサービスＩＤを、当該指紋データおよび登録ＩＤと関連付けてデータベース中に記憶するステップと、その後に、前記サーバから、ユーザコンピュータにより伝達された指紋データおよびユーザＩＤと、事業者ＩＤおよび／またはサービスＩＤとを受理することに応答して、当該指紋データと、前記データベース中の、当該ユーザＩＤに関する指紋データとを照合するステップと、前記照合結果を、前記サーバに伝達するステップとを備えたことを

特徴とするユーザ認証方法により達成される。

【０００８】本発明によれば、ユーザはいったんＦＰＤを入手すれば、これを利用して、事業者やそのサービスとの取引の際に、認証側のサーバ（認証サーバ）に指紋データを登録し、かつ、実際の取引の際に、上記事業者等のサーバ（事業者サーバ）に指紋データを伝達し、事業者サーバが、その照合を認証サーバに依頼すれば、指紋によるユーザ認証を実現することができる。これにより、ユーザも幾種類ものＦＰＤを入手する必要なく、かつ、事業者も認証自体を実行する必要が無くなる。したがって、ユーザや事業者の負担を減じることが可能となる。

【０００９】本発明の好ましい実施態様においては、さらに、前記サーバから、予め指紋照合精度を示す情報を受理し、前記データベースに記憶する際、および／または、指紋データを照合する際に、前記指紋照合精度にしたがって処理を実行する。たとえば、オンラインバンキングでは、他人誤認率を小さく設定することができるため、取引の態様にしたがった照合精度を設定することができる。

【００１０】本発明の別の実施態様において、ユーザ認証方法は、ユーザコンピュータから、事業者或いは当該事業者の運営するサービスに関するサーバに取引の申請があった場合に、当該サーバから、取引申請者であるユーザのユーザＩＤとともに、当該ユーザの登録の申請を受理するステップとを備え、前記申請の受理に応答して、当該ユーザがＦＰＤを所持しているか否かを判断して、所持していない場合には、（ａ）当該ＦＰＤを付与するステップと、（ｂ）ＦＰＤを利用した指紋データの登録のための登録ＩＤを付与するステップと、（ｃ）ユーザコンピュータから、登録ＩＤとともにＦＰＤを利用して取得した指紋データを受理するステップと、（ｄ）前記ユーザＩＤとともに、前記事業者に関する事業者ＩＤ、および／または、事業者の運営するサービスのサービスＩＤを、当該指紋データおよび登録ＩＤと関連付けてデータベース中に記憶するステップとを実行し、既に、ユーザがＦＰＤを所持しており、かつ、上記ステップ（ａ）～（ｄ）により指紋データをデータベース中に登録している場合には、（ｅ）前記取引の申請に添付された、ユーザを一意的に特定できる登録ＩＤに基づき、データベースを検索して、前記登録ＩＤに関連付けられたデータを見出すステップと、（ｆ）新たな申請にかかるユーザＩＤとともに、新たな申請にかかる事業者ＩＤおよび／またはサービスＩＤを、前記登録ＩＤに関する指紋データと関連付けて前記データベース中に記憶するステップとを実行し、その後に、前記サーバから、認証の依頼とともに、ユーザコンピュータにより伝達された指紋データおよびユーザＩＤと、事業者ＩＤおよび／またはサービスＩＤとを受理することに応答して、当該指紋データと、前記データベース中の、当該ユーザＩＤに関する指紋データとを照合するステップと、前記照合結果を、前記サーバに伝達するステップとを備えている。

【００１１】この実施態様によれば、ユーザは一度指紋データを登録しておけば、他の事業者やサービスとの取引に先立って、再度、指紋データの登録をする手順を省略することが可能となる。すなわち、ユーザの手順をより簡素化することが可能となる。

【００１２】上記認証の運用にあたって、前記サーバからの登録申請のたびに、前記サーバを所有する事業者或いは事業者が運営するサービスに対する初期経費を課金するステップと、前記サーバからの認証の依頼のたびに、前記事業者或いは前記サービスに対する認証費用を課金するステップとが設けられるのが好ましい。たとえば、認証サーバの側において、ＦＰＤの費用やその付与の費用を負担すれば、ユーザには何ら負担を課すことなく、かつ、事業者の側もＦＰＤに関する費用を負担を課すことなく、認証システムを運用することが可能となる。したがって、指紋データによるユーザの認証を普及でき、不正な商取引を有効に防止することが可能となる。

【００１３】また、本発明の目的は、少なくとも一以上の、事業者或いは事業者の運営するサービスに関する事業者サーバと、前記事業者サーバと接続され、ユーザの指紋データの登録およびその認証を実行する認証サーバとを備えた認証システムであって、前記事業者サーバが、ユーザからの登録申請があった場合に、当該ユーザにユーザＩＤを付与するユーザＩＤ付与手段と、前記ユーザＩＤとともに、前記事業者を特定する事業者ＩＤおよび／または前記サービスを特定するサービスＩＤを前記認証サーバに伝達するＩＤ伝達手段とを有し、前記認証サーバが、ユーザに登録ＩＤを付与する登録ＩＤ付与手段と、前記登録ＩＤとともにユーザから伝達された指紋データを、前記ユーザＩＤと、前記事業者ＩＤおよび／または前記サービスＩＤと関連付けて記憶するデータベースと、前記事業者サーバとユーザとの取引の際に、前記ユーザから事業者サーバに伝達された指紋データと、ユーザＩＤと、事業者ＩＤおよび／またはサービスＩＤとを受理して、当該指紋データと、データベース中の、前記ユーザＩＤと事業者ＩＤおよび／またはサービスＩＤとにより特定される指紋データとを照合する照合手段とを有し、前記照合結果が、事業者サーバに伝達されるように構成されたことを特徴とする認証システムによっても達成される。

【００１４】上記発明の好ましい実施態様においては、認証サーバが、さらに、前記事業者ＩＤおよび／またはサービスＩＤに対応して、認証照合精度を示すデータを記憶する照合精度記憶手段を有し、前記データベースへの指紋データの記憶の際、および／または、前記照合手段による照合の際に、前記照合精度記憶手段に記憶されている照合精度にしたがった処理を実行するように構成

されている。また、本発明の目的は、上記認証システムにおける、指紋データの登録および照合を実行する認証サーバや、前記認証システムと接続された事業者サーバによっても達成される。

【００１５】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態につき説明を加える。図１は、本発明の第１の実施の形態にかかる認証システムの概略を示すブロックダイヤグラムである。図１に示すように、第１の実施の形態にかかる認証システム１０は、事業者サーバ１２と、認証センターサーバ１４（以下、「認証サーバ」と称する。）と、ユーザコンピュータ１６とから構成される。これらサーバとコンピュータとの間は、インターネット１８により接続されている。なお、図１においては、ユーザコンピュータシステム１６を一つだけ示したが、インターネット１８には、多数のユーザコンピュータが接続されている。また、図１においては、事業者サーバ１２を一つだけ図示したが、インターネットには、複数の事業者サーバ１２が接続されている。

【００１６】事業者サーバ１２は、電子商取引の決済を行なうカード会社や銀行などにより運営される。認証サーバ１４は、事業者ごとに、ユーザの認証情報を蓄積する大規模データベースを有している。したがって、ユーザの認証は、実際には認証サーバ１４にて実行される。図２は、あるユーザが、ある事業者との間で取引を開始する際に実行される手順を示す図である。図２に示す例は、ユーザが、初めて、本実施の形態にかかる認証システム１０を利用する場合を示している。

【００１７】図２に示すように、ユーザは、ユーザコンピュータ１４を操作して、取引を開始したい事業者の事業者サーバ１２と接続する（ステップ２０１）。次いで、ユーザコンピュータ１６から事業者サーバ１２に、取引の申請を示すデータが伝達される（ステップ２０２）。このデータには、ユーザの住所、氏名、年齢、Ｅメールアドレス、カード番号或いは口座番号が含まれる。

【００１８】事業者サーバ１２においては、データの受理に応答して、ユーザに、固有のユーザＩＤを付与し、これをユーザコンピュータ１６に伝達する（ステップ２１１）。次いで、事業者サーバ１２は、認証サーバ１４に、ユーザ（顧客）の登録申請を示すデータを伝達する（ステップ２１２）。この登録申請を示すデータ（登録申請データ）には、予め事業者と認証センターとの間で取り極められた事業者ＩＤ、当該事業者のサービスを特定するサービスＩＤ、ユーザの住所、氏名、Ｅメールアドレス、ユーザＩＤなどが含まれる。サービスＩＤを設けたのは、同一の事業者が、複数のサービスを提供している場合があることを考慮したものである。

【００１９】認証サーバ１４は、申請データを受理すると（ステップ２２１）、ユーザＩＤを参照して、当該ユーザＩＤをもつユーザにＦＰＤを既に発送しているかどうかを判断し、次いで、事業者ＩＤにしたがって、大規模データベース中の、当該事業者ＩＤおよびサービスＩＤに関連付けられた領域に、新たな顧客に関するデータ領域を確保し、当該データ領域に、ユーザの住所、氏名およびユーザＩＤ、クレジットカード番号或いは口座番号などを格納する（ステップ２２２）。次いで、認証サービスセンターにおいては、ＦＰＤ（Finger Print Device:指紋認識装置）を、ユーザ宛てに発送する（ステップ２２３）。発送するＦＰＤには、登録時にユーザが入力する事業者ＩＤ、サービスＩＤを同封する。また、認証サーバ１６は、ユーザが登録時に使用する登録パスワード２２４を、ユーザのＥメールアドレス宛てに送信する（ステップ２２４）。なお、本実施の形態では、ユーザＩＤをステップ２１１にてユーザコンピュータ１６に伝達しているが、これに限定されるものではなく。このステップ２１１を省略し、認証サービスセンターが、ＦＰＤを発送する際に、ユーザＩＤを同封しても良い。

【００２０】ユーザがＦＰＤを受理すると、これを利用して、図３に示す手順で、自己の指紋を認証サーバ１４に登録する。まず、ユーザはＦＰＤをユーザコンピュータ１６取り付け、これを利用して指紋を読み取らせる（ステップ３０１）。ＦＰＤ３０は、たとえば、図４に示すように、マウスや他の形状をもち、かつ、プリズムや光源などの光学部材３１およびＣＣＤ３２を有する読み取り装置本体３４と、装置本体３４とケーブル３６を介して接続され、装置本体３４から供給されたデータを受理して、指紋を示すデータを生成する処理回路３８とを有している。たとえば、ＰＦＤとして、本出願人が販売するマウス型のＦＰＤ（商品名「ＥｙｅＤ　マウスＩＩ」：「ＥｙｅＤ」は商標）や、据え置き型のＦＰＤ（商品名「ＥｙｅＤ　ハムスター」：「ＥｙｅＤ」は商標）を利用することができる。

【００２１】処理回路３８は、ＣＣＤ３２からの信号を受理して、これをディジタルデータに変換するＤ／Ａ変換機４０と、ディジタルデータを一時的に記憶するバッファ４２と、バッファ４２に記憶されたデータに基づき、指紋の特徴点を抽出して、当該特徴点を利用してデータを圧縮するデータ圧縮回路４４とを有している。このような構成を備えたＦＰＤ３０を利用することにより、ユーザの指紋を示す指紋データを得ることができる。

【００２２】ＦＰＤ３０を利用した指紋データの取得の後、ユーザはコンピュータ１６を操作して、認証サーバ１６と接続する（ステップ３０２）。次いで、ユーザコンピュータ１６は、必要なデータとともに指紋データを認証サーバ１４に送信する（ステップ３０３）。上記必要なデータには、事業者サーバ１２および／または認証サーバ１６から与えられた事業者ＩＤ、サービスＩＤ、ユーザＩＤおよび登録パスワードが含まれる。

【００２３】認証サーバ１４は、これらデータを受理すると（ステップ３１１）、これを、事業者ＩＤ、サービスＩＤ、ユーザＩＤなどと関連付けて、データベース中の所定の領域に記憶する（ステップ３１２）。これにより、ある事業者のあるサービスを利用するユーザの指紋データの登録が完了する。次いで、認証サーバ１４は、事業者ＩＤに基づき、所定の事業者サーバ１２に、サービスＩＤ、ユーザＩＤおよび登録が終了したことを示すデータを伝達する（ステップ３１３）。

【００２４】このようにして、ユーザ登録が終了した後に、ユーザは、事業者との間の取引が可能となる。図５は、ユーザと事業者との間の取引、および、ユーザ認証の手順を示す図である。図５は、たとえば、事業者との間で商品の購入をする場合の例を示している。まず、ユーザコンピュータ１６と事業者サーバ１２との間で、商品の選択、価格の確認など必要な処理が実行される（ステップ５００、５１０）。この例では、ユーザＩＤやユーザのクレジットカード番号など必要な情報は、既に事業者サーバ１２に伝達されていると考える。次いで、事業者サーバ１２からユーザコンピュータ１６に対して、ユーザ認証を促す情報が与えられるのに応答して、ユーザはＦＰＤ３０を利用して、自己の指紋を読み取らせる（ステップ５０１）。読み取られた指紋から得られた指紋データは、ユーザコンピュータ１６から事業者サーバ１２に伝達される（ステップ５０２）。

【００２５】事業者サーバ１２は、指紋データ等を受理すると（ステップ５１１）、自己の事業者ＩＤ、ユーザと事業者との間の取引に対応するサービスのサービスＩＤ、取引中のユーザのユーザＩＤおよび受理した指紋データを認証サーバ１４に伝達する（ステップ５１２）。認証サーバ１４は、上記データを受信すると（ステップ５２１）、受理した事業者ＩＤ、サービスＩＤおよびユーザＩＤに基づき、データベース中に登録した指紋データを特定する。次いで、認証サーバ１４は、ステップ５２１にて受理した指紋データと、データベース中の指紋データとを照合する（ステップ５２２）。ユーザの適否、すなわち、正当なユーザであるか否かが判断されると、認証サーバ１４は、上記ユーザの適否を示す適否情報を事業者サーバ５１３に伝達する（ステップ５２３）。このようにして、事業者サーバ１２は、アクセスしたユーザの適否を知ることが可能となる。事業者サーバ１２により受理された適否情報（ステップ５１３参照）に基づき、その結果がユーザコンピュータ１６に通知される（ステップ５１４）。

【００２６】たとえば、正当なユーザであると認証された場合には、取引が継続される。その一方、正当なユーザでないと判断された場合には、事業者サーバ１４からユーザコンピュータ１２に対して、以後の処理の拒否が通知される。図２に示す手順では、ユーザが、何れかの事業者のサービスの利用、初めて申請する場合に実行される。つまり、ユーザがＦＰＤを持っていないため、事業者サーバからの申請に応答して、認証サービスセンターが、ユーザにＦＰＤを発送している（ステップ２２３参照）。これに対して、いったんユーザにＦＰＤが発送され、ユーザがこれを保持している場合には、図２のステップ２２２において、認証サーバ１４は、供給されたユーザＩＤをもつユーザにＦＰＤを既に発送していると判断する。この場合には、認証サービスセンターは、ステップ２２３を省略する。

【００２７】次に、上記構成の認証システムの運用例につき説明を加える。本実施の形態においては、このシステムを運用するのに際して、ユーザ側の負担を最小限にするように、図６に概略的に示すような課金体系としている。まず、初めてシステムを利用するユーザにＦＰＤを発送する際に生じる費用（ＦＰＤ自体の費用、および、その送付に必要な費用）は、認証サービスセンターが負担する（図６の①参照）。その一方、ユーザがある事業者のあるサービスを利用するために取引申請したとき（図６の②－１参照）、当該事業者からユーザの登録申請を受けると（図６の②－２参照）、認証サービスセンターは、申請した事業者に対して、初期経費を課金する（図６の②－３参照）。

【００２８】さらに、ユーザと事業者とが取引を行なう（図６の③－１参照）ごとに、事業者は認証サービスセンターに対して、ユーザ認証を申請する必要がある（図６の③－２参照）。このユーザ認証の申請ごとに、認証サービスセンターは、申請した事業者に対して、認証費用を課金する（図６の③－３参照）。たとえば、初期経費をＦＰＤ自体の費用の１／１００程度、認証費用を、さらにその１／１０程度とすれば、事業者にとっても過大な負担となることはない。特に、認証自体およびＦＰＤの管理等を認証サービスセンターに一元化することにより、事業者の負担を著しく軽減することが可能となる。

【００２９】次に、本発明の第２の実施の形態につき説明を加える。第２の実施の形態においては、ユーザが、一度、ある事業者との取引を申請し、認証サービスセンターから送られたＦＰＤを利用して、認証サーバ１４への指紋データの登録が終了した場合には、他の事業者或いは他のサービスを利用したい場合に、指紋データの登録を必要としない。すなわち、本システムを初めて利用するユーザは、図２に示すように、ある事業者（無論、この事業者は、認証サービスセンターを利用している事業者に限られることはいうまでもない）のあるサービスを利用したい場合に、当該事業者に対して取引を申請する（ステップ２０１、２０２参照）。これに応答して、最終的には、ＦＰＤがユーザに送られる（ステップ２２３参照）とともに、登録パスワードがユーザのもとに届く（ステップ２０４）。この登録パスワードは、第1の実施の形態と同様に、オフラインで（たとえば、ＦＰＤ

に同封されて）ユーザに届くようにしても良いし、図２に示すように、オンライン（たとえば電子メール）にて届くようにしても良い。

【００３０】次いで、ユーザは、図３に示すように、パスワードおよび指紋データなどが認証サーバに伝達され（ステップ３０３参照）、認証サーバ１４において指紋データが登録され、事業者サーバに、登録されたユーザＩＤやサービスＩＤが通知される。これにより、図５に示すような取引が、当該事業者とユーザとの間で可能となる。

【００３１】その一方、ユーザが他の事業者のサービス、或いは、同じ事業者でも他のサービスを利用したい場合には、図７に示す処理が実行される。ユーザは、入力装置を操作して、ユーザコンピュータ１６と事業者サーバ１２とを接続させた（ステップ７０１）後に、認証サービスセンターから付与された登録ＩＤを添付して、取引を申請する（ステップ７０２）。事業者サーバ１２は、これに応答して、ユーザＩＤを付与して、これをユーザコンピュータ１６に伝達する（ステップ７１１）とともに、ユーザコンピュータ１６から与えられた登録ＩＤを添付して、ユーザ（顧客）登録の申請を示す情報を、認証サーバ１４に伝達する（ステップ７１２）。

【００３２】認証サーバにおいては、当該申請を受理すると（ステップ７２１）、添付された登録ＩＤに基づき、この登録ＩＤを有するユーザに関するデータを、データベースから検索する（ステップ７２２）。このようにして、データベースにおけるユーザの指紋データを、登録を申請した事業者の事業者ＩＤやサービスＩＤおよび当該サービスに関するユーザＩＤと関連付けるような処理を実行して、当該ユーザに関する顧客情報を更新する（ステップ７２３）。このようにして、指紋データと新たな事業者のサービスでのユーザＩＤとの関連付けが終了すると、認証サーバ１４は、登録されたユーザＩＤやサービスＩＤを事業者サーバに伝達する（ステップ７２４）。事業者サーバ１２が認証サーバ１４から上記データを受理することにより（ステップ７１３）、これ以後、ユーザは、当該事業者サーバ１２を運営する事業者のサービスを利用して取引をすることが可能となる（たとえば、図５参照）。なお、第２の実施の形態においても、システムにおける費用負担や課金（ＦＰＤ費用負担、初期経費課金および認証費用の課金）は、図６に示すように実現するのが望ましい。

【００３３】本実施の形態によれば、取引申請のために、最初に一度だけ、指紋データを認証サーバに登録すれば、他の事業者のサービス等を利用する際の登録には、指紋データの登録を省略することが可能となる。これにより、より一層、ユーザの手順を簡略化することが可能となる。

【００３４】本発明は、以上の実施の形態に限定されることなく、特許請求の範囲に記載された発明の範囲内で、種々の変更が可能であり、それらも本発明の範囲内に包含されるものであることは言うまでもない。たとえば、前記第1の実施の形態においては、事業者或いは事業者のサービスごとに、認証センターにユーザは指紋データを登録している。この場合に、事業者ごとに或いはサービスごとに、指紋照合精度を変更することも可能である。これは、事業者の側において予め認証サーバに、指紋照合精度を伝達しておき、認証サーバが、指紋データの登録時、或いは、指紋データの照合時に、その照合制度にしたがった処理を実行することにより実現される。たとえば、バンキングサービスにおいては、本人以外を認証することを避けることが第１であるため、他人誤認率を低くすれば良い。

【００３５】また、前記第２の実施の形態において、既に指紋データが登録されているか否かを、ユーザが入力した登録ＩＤに基づき判断しているが、これに限定されるものではない。たとえば、ユーザがユーザコンピュータを操作して、住所、氏名、電話番号等を事業者サーバに伝達し、事業者サーバから認証サーバに、上記ユーザに関する情報が与えられ、これにより、ユーザの指紋データが既に登録されているか否かを判断しても良い。

【００３６】さらに、前記実施の形態においては、光学式のＦＰＤを利用しているがこれに限定されるものではなく、半導体式など他の形式のＦＰＤを利用可能であることは言うまでもない。なお、本明細書において、一つの手段の機能が、二つ以上の物理的手段により実現されても、若しくは、二つ以上の手段の機能が、一つの物理的手段により実現されてもよい。

【００３７】

【発明の効果】本発明によれば、ユーザに負担をかけることなく、指紋照合装置を利用した認証システムを提供することが可能となる。また、本発明によれば、事業者にも過度な負担を生じさせることなく、このため、指紋照合装置による確実な認証を広く普及させることが可能となる。これにより、電子商取引による不正を確実に防止できる。

【図面の簡単な説明】

【図１】　図１は、本発明の第１の実施の形態にかかる認証システムの概略を示すブロックダイヤグラムである。

【図２】　図２は、本実施の形態において、あるユーザが、ある事業者との間で取引を開始する際に実行される手順を示す図である。

【図３】　図３は、本実施の形態において、あるユーザが、ある事業者との間で取引を開始する際に実行される手順を示す図である。

【図４】　図４は、本実施の形態において利用されるＦＰＤの構成を示すブロックダイヤグラムである。

【図５】　図５は、本実施の形態におけるユーザと事業者との間の取引、および、ユーザ認証の手順を示す図で

ある。

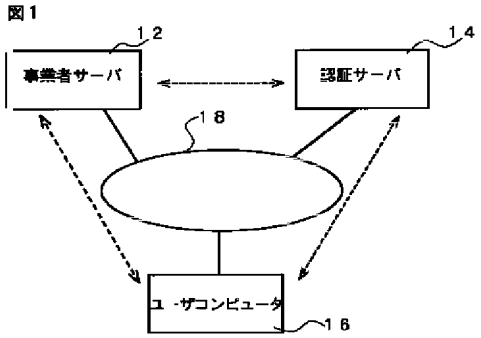
【図６】　図６は、本実施の形態にかかるシステムにおける費用負担および課金を説明するための図である。

【図７】　図７は、本発明の第２の実施の形態において、あるユーザが、ある事業者との間で取引を開始する際に実行される手順を示す図である。

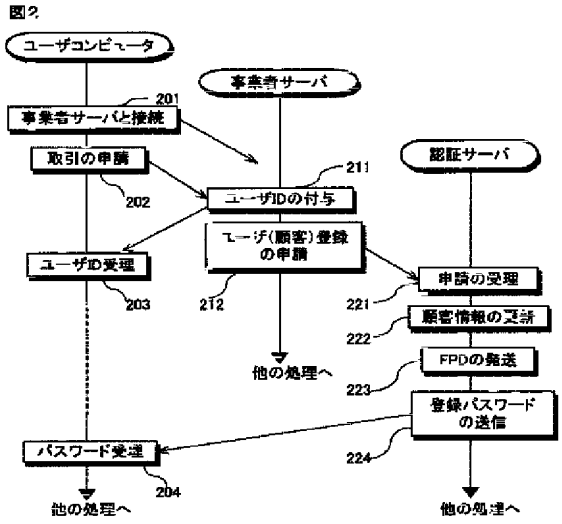
【符号の説明】

１０	認証システム
１２	事業者サーバ
１４	認証サーバ
１６	ユーザコンピュータ
３０	ＦＰＤ
３４	ＦＰＤ装置本体
３８	処理回路

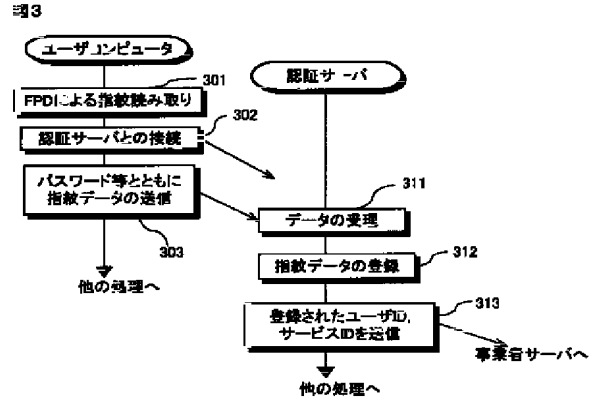
【図１】



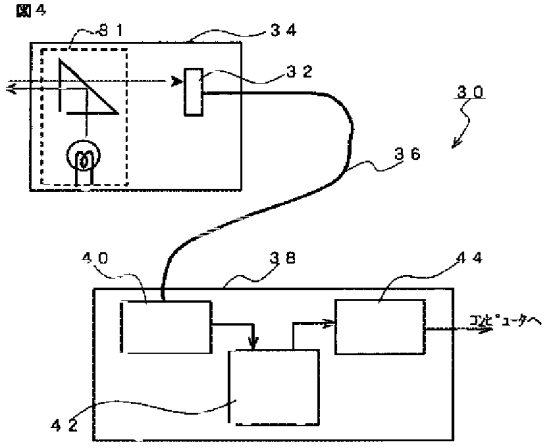
【図２】



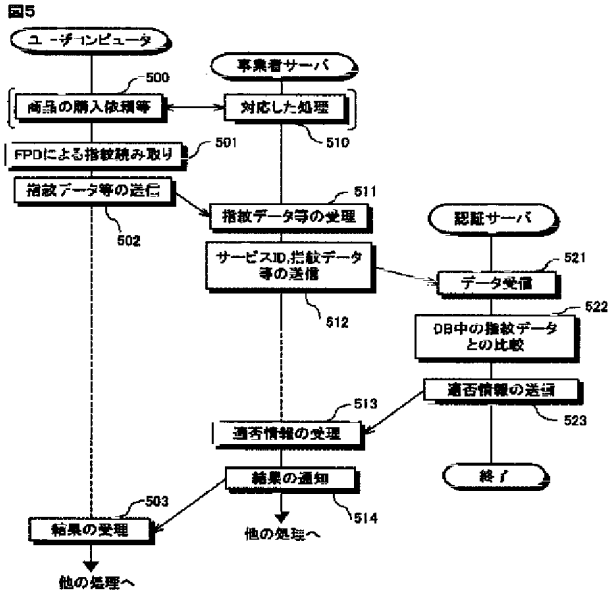
【図３】



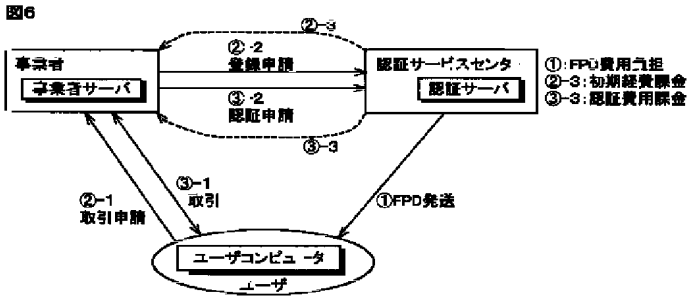
【図４】



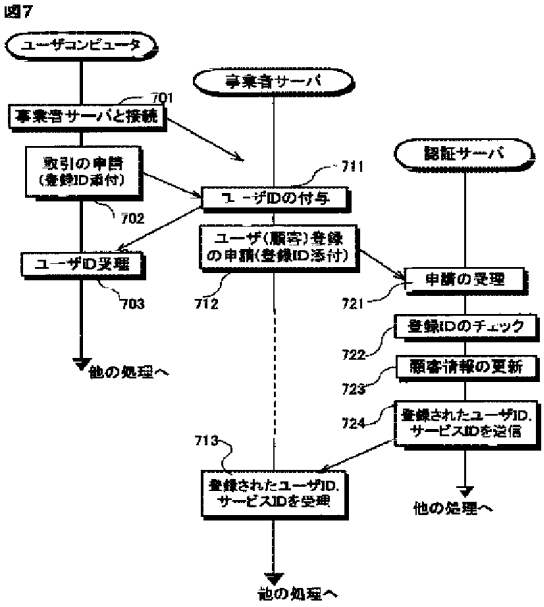
【図5】



【図6】



【図7】



フロントページの続き

(72)発明者　秋葉　茂隆
東京都千代田区内幸町２－２－３　日比谷国際ビル18F日本セキュアジェネレーション　株式会社内

Fターム(参考)　5B049 AA05 BB00 CC00 CC39 DD05 EE05 EE10 FF09 GG02 GG04 GG07
5B085 AA08 AC04 AE02 AE03 AE23 AE26 BE07 BG07